(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
25 janvier 2001 (25.01.2001)

PCT

(10) Numéro de publication internationale
WO 01/06702 A1

(51) Classification internationale des brevets[7]: H04L 9/32, G07F 7/10

(21) Numéro de la demande internationale: PCT/FR00/02075

(22) Date de dépôt international: 19 juillet 2000 (19.07.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/09396 20 juillet 1999 (20.07.1999) FR

(71) Déposants *(pour tous les États désignés sauf US)*: **FRANCE TELECOM** [FR/FR]; 6, Place D'Alleray, F-75015 Paris (FR). **LA POSTE** [FR/FR]; 4, Quai du Point du Jour, F-92777 Boulogne-billancourt (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)*: **REMERY, Patrick** [FR/FR]; 43, Rue de Cornouailles, F-14000 Caen (FR). **De SOLAGES, Aymeric** [FR/FR]; 6, Rue de la Haie Vigné, F-14000 Caen (FR). **TRAORE, Jacques** [FR/FR]; 84, Rue Abbé Lecornu, F-61100 Flers (FR).

(74) Mandataire: **POULIN, Gérard**; Société de Protection des Inventions, 3, Rue du Docteur Lancereaux, F-75008 Paris (FR).

(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)*: brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée:
— *Avec rapport de recherche internationale.*
— *Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD FOR CARRYING OUT AN ELECTRONIC TRANSACTION USING SEVERAL SIGNATURES

(54) Titre: PROCEDE DE REALISATION D'UNE TRANSACTION ELECTRONIQUE UTILISANT PLUSIEURS SIGNATURES

(57) Abstract: The invention concerns a method for carrying out an electronic transaction using several signatures, characterised in that the entities (or actors) are distributed in a communication network and share keys. A message is encapsulated inside several cryptograms, and the intermediate entities gradually decapsulate the cryptograms received. The invention is applicable to all electronic transactions, in particular to the electronic wallet.

(57) Abrégé: Selon l'invention, des entités (ou acteurs) sont réparties dans un réseau de communication et partagent des clés. Un message est encapsulé à l'intérieur de plusieurs cryptogrammes, et les entités intermédiaires décapsulent progressivement les cryptogrammes reçus. Applications à toutes les transactions électroniques, notamment au porte-monnaie électronique.

WO 01/06702 A1

PROCEDE DE REALISATION D'UNE TRANSACTION ELECTRONIQUE UTILISANT PLUSIEURS SIGNATURES

DESCRIPTION

Domaine technique

La présente invention a pour objet un procédé de réalisation d'une transaction électronique utilisant plusieurs signatures.

Elle trouve une application dans toutes les transactions (téléachat, télépaiement, accès à un service, etc...) s'effectuant à l'aide de moyens électroniques, comme les cartes à puces par exemple. L'invention trouve une application particulière dans le porte-monnaie électronique.

Etat de la technique antérieure

La sécurité des transactions électroniques par carte à puce repose sur des techniques cryptographiques. Le processeur de la puce calcule et émet une signature numérique de la transaction qui constitue une preuve de l'accord de la partie émettrice de la signature sur cette transaction. Cette preuve est spécifique à l'organisme émetteur gestionnaire de l'application. Cette signature numérique est le résultat d'un calcul portant sur les données identifiant l'émetteur de la carte, le terminal, le numéro de la transaction, le montant de la transaction et éventuellement le numéro de compte du porteur.

Les données sont transmises à l'émetteur de la carte qui effectue les traitements appropriés tels que l'audit de la transaction par vérification de la signature, mise en recouvrement, débit du compte

client, crédit du compte du fournisseur de services, etc...

Dans une des techniques antérieures décrites dans FR-A-2 748 591, la carte produit deux signatures, la première dite "longue" (algorithme à clé publique) et destinée au fournisseur de services, et la seconde, dite "courte" (algorithme à clé secrète) encapsulée dans la première est destinée à l'émetteur. Le prestataire de services vérifie la signature longue, et si le résultat est correct, rend le service commandé et stocke la signature courte. Il transmet à l'émetteur, en fin de journée, les signatures courtes stockées et les données correspondantes.

Ce schéma, s'il a l'avantage d'être simple, pose cependant quelques problèmes lorsque les paiements sont réalisés au moyen d'un porte-monnaie électronique (PME en abrégé). Il est, en effet, parfois nécessaire d'introduire un ou plusieurs acteurs intermédiaires entre les trois parties déjà citées à savoir le porteur, le prestataire de services et l'émetteur, selon les besoins de concentration effectuant des cumuls de valeur électronique.

Une solution consiste à ajouter des moyens intermédiaires appelés SAM ("Secure Application Modules) vérifiant l'une des deux signatures produites par la carte et cumulant la valeur électronique reçue.

Si les SAM intermédiaires étaient capables d'effectuer la même vérification que celle faite par l'émetteur, la sécurité serait dégradée. En effet, si l'algorithme cryptographique utilisé pour produire la signature destinée à l'émetteur de la carte était à clé secrète, la clé de l'émetteur serait placée à des

niveaux de responsabilité inférieurs vis-à-vis de la garantie de la monnaie électrique.

Si la deuxième signature destinée au fournisseur de services était produite par un algorithme à clé publique, alors les SAM intermédiaires seraient, tout comme le fournisseur de services, en mesure d'authentifier n'importe qu'elle transaction émanant d'un PME. Toutefois, dans ce cas de figure, les signatures seraient de taille nettement plus longues et donc plus coûteuses à transférer, à stocker et à vérifier.

La présente invention a justement pour but de remédier à ces inconvénients.

Exposé de l'invention

A cette fin, l'invention propose un procédé utilisant plusieurs signatures, avec une chaîne d'encapsulations-décapsulations. On suppose qu'on est en présence d'un réseau de communications (par exemple un réseau téléphonique) reliant des entités susceptibles de communiquer entre elles, avec la contrainte qu'il n'existe pas de canal de communication directe entre deux entités souhaitant communiquer et que les canaux de communication existants peuvent être unidirectionnels.

Une transaction fait intervenir un sous-ensemble d'entités appelées aussi "acteurs", concourant à des titres divers à la réalisation de la transaction. En pratique, ces entités ou acteurs sont constituées par des moyens physiques : terminal, carte, microprocesseur, etc...

Au cours de la transaction :

- une entité i dispose des moyens nécessaires (E_{ij}) au calcul des cryptogrammes destinés à une entité j, et/ou à la vérification de cryptogrammes en provenance de j,
- et une entité j dispose également des moyens (E_{ji}) corresponants,

ces moyens E_{ij} et E_{ji} ayant été obtenus au cours de la phase dite d'initialisation (effectuée préalablement et/ou parallèlement à la transaction elle-même). On dira alors que ces deux entités partagent un système de clés noté $K_{ij}=K_{ji}=\{(i,E_{ij}),(j,E_{ji})\}$. Par exemple :

- dans le cas d'un système à clés secrètes, on a : $E_{ij}=E_{ji}=S_{ij}$;
- dans le cas d'un système à clés publiques, on a :
  - pour une communication monodirectionnelle $E_{ij}=(S_i,P_i)$, et $E_j=(P_i)$,
  - pour une communication bidirectionnelle $E_{ij}=(S_i,P_i,P_j)$, et $E_{ji}=(S_j,P_i,P_j)$.

Avec cette définition, le système de clés est une notion symétrique par rapport à i et j. En revanche, si l'on note $K_{ij}(m)$ le cryptogramme d'un message m envoyé par i à j, on a $K_{ij}(m)\neq K_{ji}(m)$.

Dans ces conditions et sous ces hypothèses, une entité source de message "encapsule" (c'est-à-dire renferme) un message dans une suite de cryptogrammes portant sur des cryptogrammes, eux-mêmes portant sur des cryptogrammes, etc... Tous ces cryptogrammes sont calculés à l'aide de systèmes de clés que l'entité source partage respectivement avec chacune des entités intermédiaires situées sur le chemin de la

communication. Le cryptogramme global est émis et chaque entité intermédiaire "décapsule" (c'est-à-dire extrait) le cryptogramme qu'elle reçoit avec le système de clés qu'elle partage avec l'entité source, et transmet le cryptogramme restant à l'entité suivante. De proche en proche, le premier cryptogramme calculé parvient à l'entité destinataire qui extrait le message qui lui est destiné à l'aide du système de clés approprié.

Selon les besoins de la transaction et les protocoles utilisés, les cryptogrammes calculés peuvent servir à l'authentification des acteurs, à l'authentification de l'origine des messages, ou à la non-répudiation (à l'émission ou à la réception) de ces messages.

Ce procédé suppose l'existence d'un système de gestion des systèmes de clés (qui englobe la génération, la distribution et/ou l'échange de clés nécessaires à l'établissement de communications sûres avec les autres acteurs), mis en oeuvre au cours d'une phase dite d'initialisation. Ce système de gestion de clés peut être quelconque et par exemple consister en une infrastructure à clé publique, avec un protocole de transport de clés associé.

Parmi les entités en présence, certaines peuvent jouer le rôle de tiers de confiance. Par exemple :

- dans le cas d'un système à clé publique, il peut s'agir d'une autorité de certification,
- dans le cas d'un système à clé secrète, il peut s'agir d'une entité maître, partageant une clé secrète avec chacune des autres entités, ou certaines d'entre elles seulement.

Une entité peut participer à une transaction à divers titres comme par exemple :

1. assurer un relais de l'information : une entité joue le rôle de relais intermédiaire et pallie ainsi l'absence de canal de communication reliant directement un expéditeur et un destinataire d'un message nécessaire à la transaction ;
2. assurer une désynchronisation : une entité joue le rôle de cache intermédiaire de messages pour le compte d'une autre entité, destinataire réel de ces messages ; cette entité intermédiaire :
   - pallie l'indisponibilité temporaire du destinataire,
   - est conçue pour être sollicitée plus fréquemment que le destinataire et joue le rôle d'interface regroupant les messages et évitant la sollicitation systématique du destinataire.

L'émetteur et/ou le destinataire ont intérêt à l'arrivée des informations à destination. Les acteurs intermédiaires doivent donc être des relais sûrs de cette information. Plusieurs cas sont notamment possibles :

- les acteurs intermédiaires ont également intérêt à l'arrivée des informations à destination. C'est le cas par exemple lorsqu'il s'agit d'un commerçant dans une transaction financière faisant intervenir un client (acteur expéditeur) et le système de gestion du moyen de paiement (acteur destinataire),
- l'expéditeur et/ou le destinataire font confiance aux acteurs intermédiaires pour

l'opération de relayage (mais pas nécessairement pour l'authenticité de l'origine des informations),

- les acteurs expéditeurs et destinataire font totalement confiance aux acteurs intermédiaires (tiers de confiance),
- les acteurs expéditeur et destinataire ne font pas du tout confiance aux acteurs intermédiaires, et des moyens de non-répudiation à l'émission et à la réception sont mis en place.

De façon précise, l'invention a pour objet un procédé de réalisation d'une transaction électronique à travers un réseau de communication reliant une pluralité d'entités, ce procédé étant caractérisé en ce qu'il comprend les opérations suivantes :

a) une première entité élabore un premier message rassemblant les données de la transaction et calcule un premier cryptogramme de ce premier message en utilisant un premier système de clés qu'elle partage avec une dernière ($n^{ième}$) entité ; la première entité associe ensuite à ce premier cryptogramme un deuxième message et calcule un deuxième cryptogramme de l'ensemble en utilisant un deuxième système de clés qu'elle partage avec l'avant-dernière $(n-1)^{ième}$ entité ; et ainsi de suite ; la première entité associe au $(n-2)^{ième}$ cryptogramme précédemment obtenu un $(n-1)^{ième}$ message et calcule un $(n-1)^{ième}$ cryptogramme de l'ensemble en utilisant un $(n-1)^{ième}$ système de clés qu'elle partage avec la deuxième entité ; la première

entité transmet le dernier cryptogramme calculé à travers le réseau de communication ;

b) la deuxième entité reçoit ce dernier cryptogramme, utilise le système de clés approprié pour extraire du $(n-1)^{ième}$ cryptogramme le $(n-1)^{ième}$ message qu'il contient, et transmet le $(n-2)^{ième}$ cryptogramme restant à la troisième entité ; et ainsi de suite ; la $n^{ième}$ entité reçoit le premier cryptogramme et utilise le système de clés approprié pour extraire le premier message qu'il contient.

Dans cette définition, la "première entité" n'est pas nécessairement l'entité source du message mais elle peut l'être. De même, la "dernière entité" n'est pas nécessairement l'entité destinataire in fine du message mais elle peut l'être. Ainsi, dans le cas particulier précédent, le réseau de communication comprend uniquement des entités partageant un système de clés avec une première entité, la transaction s'effectuant alors entre la première entité, qui est la source du message et la dernière, qui est le destinataire du message.

L'encapsulation est alors totale à la source et la décapsulation progressive jusqu'au destinataire.

Dans une variante de mise en oeuvre, l'encapsulation est partagée (ou répartie). Dans ce cas, le réseau de communication comprend un premier groupe d'entités constitué d'une première entité et de (i-1) autres partageant chacune un système de clés avec ladite première entité, et un deuxième groupe d'entités constitué d'une première entité qui est la dernière

entité du premier groupe à savoir l'entité i, et de (n-i) autres. L'entité i partage un système de clés avec chacune de ses (n-i) entités suivantes. Ce procédé comprend deux phases successives :

- une première phase dans laquelle le message élaboré par la première entité du premier groupe est transmis à la $i^{ème}$ entité du premier groupe conformément aux opérations a) et b) définies plus haut,
- une seconde phase dans laquelle le message extrait par la première entité du second groupe est transmis à la dernière entité du second groupe conformément auxdites opérations a) et b).

Dans un cas général, on peut combiner les modes de mise en oeuvre qui viennent d'être définis. Ainsi, le réseau de communications peut comprendre un premier groupe d'entités constitué d'une première entité et de (i-1) autres partageant un système de clés avec ladite première entité, un deuxième groupe d' entités constitué d'une première entité, qui est la dernière entité du premier groupe et (j-i+1) autres partageant un système de clés avec ladite première entité du deuxième groupe, un troisième groupe d'entités constitué d'une première entité qui est la dernière entité du deuxième groupe et de (n-j) autres, les (n-j+1) entités de ce troisième groupe partageant un système de clés avec la première entité du premier groupe, ce procédé étant caractérisé en ce que :

- la première entité du premier groupe effectue les opérations a) définies plus haut, avec les systèmes de clés qu'elle a en commun avec

chacune des autres entités du premier et du troisième groupe,

- les entités du premier groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) définies plus haut,
- la première entité du deuxième groupe effectue les opérations a) avec les systèmes de clés qu'elle a en commun avec chacune des autres entités du deuxième groupe,
- les entités du deuxième groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) définies plus haut,
- les entités du troisième groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b).

La présente invention a également pour objet une application de ce procédé au paiement par porte-monnaie électronique.

Description détaillée de modes de mise en oeuvre

L'authenticité des données est obtenue par des techniques mettant en oeuvre des mécanismes de chiffrement, d'authentification ou de signature.

Le terme "signature" utilisé dans la suite désigne des cryptogrammes obtenus aussi bien au moyen de mécanismes de signature basés sur des algorithmes à clé publique (avec recouvrement ou non du message) que ceux basés sur des algorithmes à clé secrète ("MAC", ou "Message Authentification Code" en anglais).

Les notations utilisées dans la suite sont les suivantes :

- m_{ij} : message déterminé par l'entité i et destiné à l'entité j. Un message déterminé par une entité i pourra très bien être vide ou identique à un message déterminé par une autre entité j ($m_{i,l}=m_{j,l}$ pour $i\neq j$ et $\underline{l}$ donné), ou encore un cryptogramme. Dans le cas du paiement par carte PME (Porte-Monaie Electronique), $m_{i,j}$ désignera par exemple les données de la transaction (y compris les éléments anti-rejeux).
- $K_{i,j}(m)$: cryptogramme du message m, calculé par i à l'aide du système de clés K_{ij}. L'algorithme de calcul de ce cryptogramme dépend de l'application. Il n'est fait aucune restriction sur l'algorithme utilisé pour le calcul de ce cryptogramme. Il pourra s'agir par exemple :
    1. d'un algorithme à clé publique (RSA, DSA, etc...) ou d'un algorithme à clé secrète (MAC-DES, etc...),
    2. d'un algorithme de signature, ou d'un algorithme de chiffrement. Dans le cas d'une signature, on suppose implicitement que le cryptogramme utilisé permet le recouvrement d'un message. Cette hypothèse n'est pas restrictive car on peut toujours remplacer $K_{ij}(m)$ par $K'_{ij}(m)=K_{ij}(m)||m$, où $||$ désigne la concaténation de messages.
- La notation $K_{ij}(X,m)$ est considérée comme équivalente à $K_{ij}(X||m)$, dans l'hypothèse où les deux parties en présence ont convenu de la longueur de X.

- Dans la suite, le message X sera lui-même un cryptogramme K(m'). On appellera "encapsulation" le fait d'utiliser ainsi un cryptogramme X=K'(m) comme message.
- Lorsque le cryptogramme $K_{ij}(X,m)$ est destiné à préserver l'intégrité du message, mais que les canaux qu'il doit emprunter sont contrôlés par des entités qui ont intérêt au transfert de X, on pourra avoir par exemple $K_{ij}(K(m'),m)=K(m')||K'_{ij}(m)$, aucune restriction n'étant faite sur l'algorithme de calcul des cryptogrammes.

Quatre exemples de mise en oeuvre de ce procédé vont être décrits

Exemple 1 : Encapsulation totale à la source et décapsulation progressive

La source élabore un message $m_{1,n}$ rassemblant les données de la transaction et calcule un premier cryptogramme $K_{1,n}(m_{1,n})$ de ce premier message en utilisant un premier système de clés $K_{1,n}$ qu'elle partage avec la dernière $n^{ième}$ entité ; la source associe ensuite à ce premier cryptogramme un deuxième message $m_{1,n-1}$ et calcule un deuxième cryptogramme $K_{1,n-1}(K_{1,n}(m_{1,n}),m_{1,n-1})$ de l'ensemble en utilisant un deuxième système de clés $K_{1,n-1}$ qu'elle partage avec une avant-dernière $(n-1)^{ième}$ entité, et ainsi de suite, ... ; la première entité associe au $(n-2)^{ième}$ cryptogramme précédemment obtenu un $(n-1)^{ième}$ message $m_{1,2}$ et calcule un $(n-1)^{ième}$ cryptogramme de l'ensemble en utilisant un $(n-1)^{ième}$ système de clés $K_{1,2}$ qu'elle partage avec une deuxième entité, et la source transmet

le dernier cryptogramme calculé à travers le réseau de communication vers l'entité 2.

On peut schématiser cette première phase par le diagramme suivant où la flèche orientée à droite symbolise le transfert d'information entre l'entité 1 (à gauche) et l'entité 2 (à droite) :

Entité 1 Entité 2

$$\xrightarrow{K_{1,2}(K_{1,3}(K_{1,4}(\ldots..(K_{1,n-1}(K_{1,n}(m_{1,n}),m_{1,n-1}),\ldots\ldots,m_{1,4}),m_{1,3}),m_{1,2})}$$

L'entité 2, qui reçoit le message de l'entité 1, réalise une décapsulation partielle de ce message à l'aide du système de clés $K_{1,2}$; elle vérifie (et conserve éventuellement) le cryptogramme qui lui est destiné (en l'occurrence la signature du message $m_{1,2}$), puis transmet à l'entité 3 le reste du message. On a donc, avec les mêmes conventions, le schéma suivant :

Entité 2 Entité 3

$$\xrightarrow{K_{1,3}(K_{1,4}(\ldots(K_{1,n-1}(K_{1,n}(m_{1,n}),m_{1,n-1}),\ldots,m_{1,4}),m_{1,3})}$$

Ce procédé est réitéré de proche en proche jusqu'à l'entité n. Pour les entités i et i+1 intermédiaires, on a :

Entité i Entité i+1

$$\xrightarrow{K_{1,i+1}(K_{1,i+2}(\ldots..(K_{1,n-1}(K_{1,n}(m_{1,n})),m_{1,n-1}),\ldots\ldots,m_{1,i+2}),m_{1,i+1})}$$

Enfin, l'avant-dernière entité (n-1) transmet au destinataire (n) le dernier cryptogramme $K_{1,n}(m_{1,n})$ et celui-ci, à l'aide du système de clés $K_{1,n}$, récupère le message qui lui était destiné :

Entité n−1 Entité n

$$\xrightarrow{K_{1,n}(m_{1,n})}$$

Exemple 2 : Encapsulation partagée

L'entité 1 partage un système de clés avec seulement une partie des entités se trouvant sur le chemin de communication, à savoir les entités 2, ..., i qui forment un premier groupe. L'entité i, quant à elle, partage un système de clés avec chacune des entités suivantes : i+1, i+2, ..., n et forme avec elles un second groupe.

L'entité 1 élabore un message pour la dernière entité i du premier groupe, soit $m_{1,i}$ et encapsule ce message avec les systèmes de clés qu'elle partage avec chacune des entités du premier groupe, et transmet le tout à l'entité 2 :

Entité 1 → Entité 2 : $K_{1,2}(K_{1,3}(K_{1,4}(.....(K_{1,i-1}(K_{1,i}(m_{1,i}).\ m_{1,i-1}).\ .....\ m_{1,4}).\ m_{1,3}).\ m_{1,2})$

Dans ce premier groupe, les entités décapsulent progressivement les cryptogrammes jusqu'à ce que l'avant-dernière entité i-1 transmette à la dernière entité i, le cryptogramme du message qui lui est destiné :

Entité i-1 → Entité i : $K_{1,i}(m_{1,i})$

L'entité i procède alors à une encapsulation de la totalité des messages $m_{i,i+1}$, $m_{i,i+2}$, ..., $m_{i,n}$ destinés aux entités du second groupe. Le contenu de ces messages peut dépendre du cryptogramme reçu. Le résultat de cette encapsulation est ensuite transmis selon le procédé déjà décrit, d'abord de l'entité i à l'entité i+1 :

Entité i → Entité i+1 : $K_{i,i+1}(K_{i,i+2}(K_{i,i+3}(.....(K_{i,n-1}(K_{i,n}(m_{i,n}),m_{i,n-1}).....m_{i,i+3}),m_{i,i+2}),m_{i,i+1})$

et ainsi de suite à travers les entités du second groupe jusqu'à l'avant dernière, n-1, qui transmet le dernier cryptogramme au destinataire n.

Exemple 3 : Cas général

L'entité 1 partage un système de clés avec une partie des entités se trouvant sur le chemin de communication, partie que pour la simplicité de l'exposé, on supposera être 2, ..., i, j+1, ..., n. L'entité 1 réalise donc une encapsulation partielle comme le montre le schéma suivant :

Entité 1 Entité 2

$K_{1,2}(.....K_{1,i}(K_{1,j+1}(.....K_{1,n}(m_{1,n}).....m_{1,j+1}),m_{1,i}).....m_{1,2})$

Chaque entité intermédiaire décapsule le message qu'elle reçoit à l'aide du système de clés approprié, et ceci jusqu'à l'entité i :

Entité i-1 Entité i

$K_{1,i}(K_{1,j+1}(.....K_{1,n}(m_{1,n}).....m_{1,j+1}),m_{1,j})$

Tout acteur (ici "i" uniquement), qui, après avoir extrait le message qui lui était destiné, obtient un reste de message destiné à un acteur non adjacent sur le parcours, le réencapsule à destination de l'entité adjacente et (éventuellement) des suivantes.

Dans cet exemple, l'entité i partage un système de clés avec chacune des entités suivantes : i+1, i+2, ..., j. L'entité i reçoit le message de i-1, réalise une décapsulation partielle, puis réencapsule le message obtenu à destination de i+1, i+2, ..., j.

Entité i Entité i+1

$K_{i,i+1}(.....K_{i,j}(K_{1,j+1}(.....K_{1,n}(m_{1,n}).....m_{1,j+1}),m_{i,j}).....m_{i,i+1})$

Chaque entité intermédiaire décapsule le message qu'elle reçoit à l'aide du système de clés et ceci jusqu'à l'entité j :

Entité j-1 Entité j

$$K_{i,j}(K_{1,j+1}(.....K_{1,n}(m_{1,n}).....,m_{1,j+1}),m_{i,j}) \longrightarrow$$

L'entité j décapsule à nouveau. Le message décapsulé est ensuite transmis de proche en proche de j+1 à n :

Entité j Entité j+1

$$K_{1,j+1}(.....K_{1,n}(m_{1,n}).....,m_{1,j+1}) \longrightarrow$$

Entité n-1 Entité n

$$K_{1,n}(m_{1,n}) \longrightarrow$$

On peut illustrer, dans le cadre de cet exemple, le cas particulier décrit précédemment dans lequel certains cryptogrammes $K_{i,j}(...)$ sont de la forme $K_{i,j}(X,m)=X,K_{i,j}(m)$. L'entité i n'encapsule pas les messages à destination de i+1, i+2, ..., j, parce que les canaux sont considérés comme sûrs et les entités impliquées n'ont pas intérêt à falsifier les messages.

Entité 1 Entité i + 1

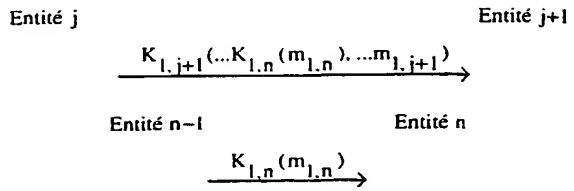
$$\xrightarrow{K_{i,i+1}(m_{i,i+1}),K_{i,i+2}(m_{i,i+2}),....,K_{i,j}(m_{i,j}),K_{1,j+1}(...K_{1,n}(m_{1,n}),....,m_{1,j+1})}$$

Chaque entité intermédiaire reçoit et contrôle le message qui lui est destiné à l'aide de son système de clés, ceci jusqu'à l'entité j.

Entité j-1 Entité j

$$\xrightarrow{K_{i,j}(m_{i,j}),K_{1,j+1}(...K_{1,n}(m_{1,n}),....,m_{1,j+1})}$$

L'entité j reçoit et contrôle le message qui lui est destiné. Le message est ensuite transmis de proche en proche de j+1 à n :



Exemple 4 : cas du porte-monnaie électronique (PME)

Dans cet exemple, les entités (ou les acteurs) sont :

- des cartes PME notées A,
- des points de service P, aptes à recevoir les cartes,
- des concentrateurs de points de service et leur module de sécurité MS,
- un émetteur E chargé d'émettre les cartes PME et chargé d'acquérir la monnaie électronique.

Le réseau de communication relie les points de service aux concentrateurs et ces concentrateurs à l'émetteur.

Par hypothèse :

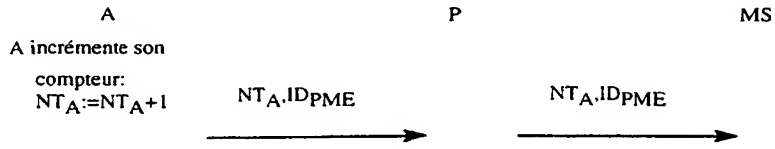
- A et MS partagent un système de clés $K_{A,M}$,
- A et E partagent un système de clés $K_{A,E}$,
- A et P partagent un système de clés $K_{A,P}$.

Les notations employées sont les suivantes :

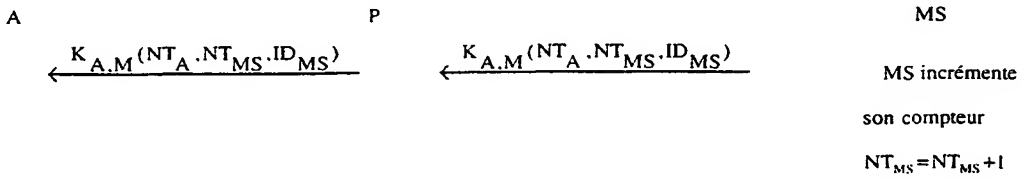
- K(m) cryptogramme du message m obtenu en utilisant le système de clés K,
- NT_A : numéro de transaction du PME A,

- NT_{MS} : numéro de transaction de MS,
- ID_{PME} : identifiant du PME,
- ID_{MS} : identifiant de MS.

Après l'étape préalable d'échange de clés, A, P et MS échangent des informations relatives au numéro de la transaction NT_A et à l'identifiant du PME :



Puis le module de sécurité communique à l'entité P son numéro de transaction NT_{MS}, après l'avoir incrémenté, ainsi que son identité ; l'identité P retransmet ces informations à l'entité A.



La carte A vérifie les données qu'elle a reçues et initialise à zéro le cumul (cumul=0).

Commence alors le cycle de consommation d'unités de service. Les opérations mises en oeuvre sont alors les suivantes :

A P

ordre de débit de montant m

cumul := cumul+m

calcul de la micro-transaction

$K_{A.P}(M.K_{A.M}(M.K_{A.E}(M'))$

où $M=(m.cumul.NT_A.NT_{MS}.ID_{MS})$

et $M'=(cumul.NT_A.NT_{MS}.ID_{MS})$

P vérifie les données qui lui ont été transmises

cumul :=cumul+m

C'est ensuite le retour au début du cycle si l'utilisation du service n'est pas terminée. En fin de session de service, on a l'ultime échange suivant :

P MS E

P ne transmet à MS que la dernière signature $K_{A.M}(M.K_{A.E}(M'))$ $K_{A.E}(M')$

REVENDICATIONS

1. Procédé de réalisation d'une transaction électronique à travers un réseau de communication reliant une pluralité d'entités, caractérisé en ce qu'il comprend les opérations suivantes :

a) une première entité élabore un premier message rassemblant les données de la transaction et calcule un premier cryptogramme de ce premier message en utilisant un premier système de clés qu'elle partage avec une dernière ($n^{ième}$) entité ; la première entité associe ensuite à ce premier cryptogramme un deuxième message et calcule un deuxième cryptogramme de l'ensemble en utilisant un deuxième système de clés qu'elle partage avec une avant-dernière $(n-1)^{ième}$ entité ; et ainsi de suite ; la première entité associe au $(n-2)^{ième}$ cryptogramme précédemment obtenu un $(n-1)^{ième}$ message et calcule un $(n-1)^{ième}$ cryptogramme de l'ensemble en utilisant un $(n-1)^{ième}$ système de clés qu'elle partage avec une deuxième entité ; la première entité transmet le dernier cryptogramme calculé à travers le réseau de communication,

b) la deuxième entité reçoit ce dernier cryptogramme, utilise le système de clés approprié pour extraire du $(n-1)^{ième}$ cryptogramme le $(n-1)^{ième}$ message qu'il contient, et transmet le $(n-2)^{ième}$ cryptogramme restant à la troisième entité ; et ainsi de suite ; la $n^{ième}$ entité reçoit le premier cryptogramme et utilise le système de clés

approprié pour extraire le premier message qu'il contient.

2. Procédé selon la revendication 1, dans lequel le réseau de communication comprend uniquement des entités partageant une clé avec une première entité, la transaction s'effectuant alors entre la première entité, qui est la source du message et la dernière, qui est le destinataire du message.

3. Procédé selon la revendication 1, dans lequel le réseau de communication comprend un premier groupe d'entités constitué d'une première entité et de (i-1) autres partageant chacune un système de clés avec ladite première entité, et un deuxième groupe d'entités constitué d'une première entité qui est la dernière entité du premier groupe à savoir l'entité i et de (n-i) autres, l'entité i partageant un système de clés avec chacune des (n-i) entités suivantes, ce procédé comprenant deux phases successives :

- une première phase dans laquelle le message élaboré par la première entité du premier groupe est transmis à la $i^{ème}$ entité du premier groupe conformément aux opérations a) et b) de la revendication 1,
- une seconde phase dans laquelle le message extrait par la première entité du second groupe est transmis à la dernière entité du second groupe conformément aux opérations a) et b) de la revendication 1.

4. Procédé selon la revendication 1, dans lequel le réseau de communication comprend un premier groupe d'entités constitué d'une première entité et de (i-1)

autres partageant chacune un système de clés avec ladite première entité, un deuxième groupe d'entités constitué d'une première entité, qui est la dernière entité du premier groupe et (j-i+1) autres partageant chacune un système de clés avec ladite première entité du deuxième groupe, un troisième groupe d'entités constitué d'une première entité qui est la dernière entité du deuxième groupe et de (n-j) autres, les (n-j+1) entités de ce troisième groupe partageant chacune un système de clés avec la première entité du premier groupe, ce procédé étant caractérisé en ce que :

- la première entité du premier groupe effectue les opérations a) de la revendication 1, avec les systèmes de clés qu'elle a en commun avec chacune des autres entités du premier et du troisième groupe,
- les entités du premier groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) de la revendication 1,
- la première entité du deuxième groupe effectue les opération a) de la revendication 1 avec les systèmes de clés qu'elle a en commun avec chacune des autres entités du deuxième groupe,
- les entités du deuxième groupe traitent les cryptogrammes qu'elles reçoivent conformément aux opérations b) de la revendication 1,
- les entités du troisième groupe décryptent les cryptogrammes qu'elles reçoivent conformément aux opérations b) de la revendication 1.

5. Procédé selon la revendication 1 dans lequel, la première entité i d'un groupe calcule un

cryptogramme des messages destinés aux autres entités i+1, i+2, ..., j du groupe, sans les encapsuler, chaque entité i+1, i+2, ..., j reçoit et contrôle le message qui lui est destiné à l'aide de son système de clé partagé avec i.

6. Procédé selon la revendication 1, dans lequel la transaction électronique est un paiement, les entités étant constituées par des cartes (A), des points de service (P) aptes à recevoir lesdites cartes (A), des concentrateurs de points de service équipés d'un module de sécurité (MS) et reliés aux points de service et un émetteur (E) chargé d'émettre des cartes de type paiement électronique et chargé d'acquérir la monnaie électronique, le réseau de communication reliant des points de service (P) aux concentrateurs et ces concentrateurs à l'émetteur, chaque carte (A) partageant avec un module de sécurité (MS) un système de clés $K_{A,M}$, chaque carte A partageant également avec l'émetteur (E) un système de clés $K_{A,E}$, chaque carte (A) partageant avec un point de service (P) un système de clés $K_{A,P}$.

7. Procédé selon la revendication 6, dans lequel :

a) la carte (A) :

- calcule un message (M') à destination de l'émetteur (E), ce message comprenant le cumul des montants payés, le numéro (NT_A) de la transaction, le numéro de transaction (NT_{MS}) du module de sécurité (MS) auquel le point de service est relié, et l'identifiant (ID_{MS}) de ce module de sécurité,

- calcule un premier cryptogramme $K_{A,E}(M')$ de ce message en utilisant le système de clés $K_{A,E}$ qu'elle partage avec l'émetteur,
- ajoute à ce premier cryptogramme un message (M) contenant le montant de la transaction (m), le cumul, les numéros (NT_A, NT_{MS}) et l'identifiant (ID_{MS}),
- encapsule le résultat dans un deuxième cryptogramme $K_{A,M}(M, K_{A,E}(M'))$ utilisant le système de clés $K_{A,M}$ qu'elle partage avec le module de sécurité (MS),
- ajoute à ce deuxième cryptogramme, le message M,
- encapsule le résultat dans un troisième cryptogramme $K_S(M, K_{A,M}(M, K_{A,E}(M')))$, en utilisant le système de clés $K_{A,P}$,
- transmet ce troisième cryptogramme au point de service (P),

b) le point de service (P) décapsule le cryptogramme reçu à l'aide du système de clés $K_{A,P}$, récupère et vérifie le message M, et enregistre $K_{A,M}(M, K_{A,E}(M'))$, le procédé étant répété si l'utilisation du service n'est pas terminée,

c) en fin d'utilisation du service le point de service (P) retransmet le dernier $K_{A,M}(M, K_{A,E}(M'))$ au module de sécurité (MS),

d) le module de sécurité (MS) décapsule le cryptogramme reçu à l'aide du système de clés $K_{A,M}$, récupère le message (M) et transmet $K_{A,E}(M')$ à l'émetteur,

e) l'émetteur (E) décapsule le cryptogramme reçu à l'aide du système de clés $K_{A,E}$ et extrait le message (M') qui lui était destiné.

INTERNATIONAL SEARCH REPORT

Internatio \pplication No
PCT/FR 00/02075

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 42610 A (PAILLES JEAN CLAUDE ;POSTE (FR); FRANCE TELECOM (FR); GIRAULT MARC) 13 November 1997 (1997-11-13) abstract page 10, line 12 -page 12, line 24 page 14, line 14 -page 15, line 15 claims 1,2 figures 6,7 ---	1-7
A	EP 0 588 339 A (NIPPON TELEGRAPH & TELEPHONE) 23 March 1994 (1994-03-23) abstract column 2, line 30 -column 5, line 46 claims 1,2 figure 5 -----	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 November 2000	15/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatio Application No
PCT/FR 00/02075

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9742610 A	13-11-1997	FR 2748591 A	14-11-1997
		EP 0909433 A	21-04-1999
		US 6105862 A	22-08-2000
EP 0588339 A	23-03-1994	JP 6103425 A	15-04-1994
		JP 6103426 A	15-04-1994
		JP 6162289 A	10-06-1994
		JP 6162287 A	10-06-1994
		JP 6161354 A	07-06-1994
		DE 69322463 D	21-01-1999
		DE 69322463 T	10-06-1999
		EP 0856821 A	05-08-1998
		EP 0856822 A	05-08-1998
		US 5396558 A	07-03-1995
		US 5446796 A	29-08-1995
		US 5502765 A	26-03-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande nationale No
PCT/FR 00/02075

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 97 42610 A (PAILLES JEAN CLAUDE ;POSTE (FR); FRANCE TELECOM (FR); GIRAULT MARC) 13 novembre 1997 (1997-11-13) abrégé page 10, ligne 12 -page 12, ligne 24 page 14, ligne 14 -page 15, ligne 15 revendications 1,2 figures 6,7 ---	1-7
A	EP 0 588 339 A (NIPPON TELEGRAPH & TELEPHONE) 23 mars 1994 (1994-03-23) abrégé colonne 2, ligne 30 -colonne 5, ligne 46 revendications 1,2 figure 5 -----	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" *document particulièrement pertinent; l'inven tion revendiquée ne peut* être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 novembre 2000	15/11/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande nationale No
PCT/FR 00/02075

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9742610 A	13-11-1997	FR 2748591 A	14-11-1997
		EP 0909433 A	21-04-1999
		US 6105862 A	22-08-2000
EP 0588339 A	23-03-1994	JP 6103425 A	15-04-1994
		JP 6103426 A	15-04-1994
		JP 6162289 A	10-06-1994
		JP 6162287 A	10-06-1994
		JP 6161354 A	07-06-1994
		DE 69322463 D	21-01-1999
		DE 69322463 T	10-06-1999
		EP 0856821 A	05-08-1998
		EP 0856822 A	05-08-1998
		US 5396558 A	07-03-1995
		US 5446796 A	29-08-1995
		US 5502765 A	26-03-1996